

RECEIVED

NOV 02 2018

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF)
WHITE IPHONE, SERIAL NUMBER)
C8PW4C4PJC6D, LOCATED AT)
324 PROSPERITY DRIVE,)
KNOXVILLE, TN 37923)

Case No. 3:18-MJ-2188

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michelle Evans, a Special Agent with Homeland Security Investigations ("HSI"),
being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent of HSI since 1995, and am currently assigned to the Office of the Resident Agent in Charge, Knoxville, Tennessee. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have conducted, coordinated, and/or participated in numerous investigations relating to the sexual exploitation of children. I have participated in numerous search warrant executions by HSI, as well as state and local police departments, and have participated in numerous seizures of computer systems and other evidence involving child exploitation and/or child pornography offenses. I have applied for and executed numerous search warrants pertaining to the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a

search warrant.

2. This affidavit is submitted in support of an application for a search warrant for a white iPhone (hereinafter "the device") owned by Joshua Young and currently located in secure evidence at the HSI office at 324 Prosperity Drive, Knoxville, Tennessee, 37923. I obtained the device from Joshua Young on August 15, 2018, at his residence when Young consented to an interview and the search of the device. The device bears the manufacturer's trade name "iPhone," is white in color, and has serial number C8PW4C4PJC6D. The device is seated in a blue case. Mr. Young acknowledged that this device is his own personal cell phone and that he uses it for Internet activity. This property is more particularly described in Attachment A which is incorporated by reference herein. The seizure and examination process to recover the digital media contained in this property, the electronically stored information (ESI) in the property, and the data stored on the smartphone is described in Attachment B, which is also incorporated by reference herein.

3. The information contained within the affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning the investigation. I have set forth only the facts which I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, pertaining to the receipt, distribution and possession of visual depictions of minors engaged in sexually explicit conduct, are presently located on the device.

GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT

4. INTERNET SERVICE PROVIDER: A company that provides its customers with access to the Internet, usually over telephone lines or cable connections. Typically, the customer pays a monthly fee, and the Internet Service Provider (ISP) supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.

5. THE INTERNET: The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across county, state, and national boundaries.

6. INTERNET PROTOCOL ADDRESS ("IP address"): The unique numeric address of a machine or computer attached to and using the Internet. This address is displayed in blocks of numbers, or blocks of numbers and letters, such as 123.456.789.001 or 2001:0DB8:AC10:FE01, just for examples. Each number can only be used by one computer or machine over the Internet at a time. Other numbers such as "mac" addresses or port numbers may further distinguish devices or machines sharing a connection, but the IP address identifies the point at which a computer or machine is connected to the Internet, normally via a modem.

7. SMART PHONE: A Smartphone, or smart phone, is a mobile phone built on a mobile operating system, with more advanced computing capability and connectivity than a feature phone. The first smartphones combined the functions of a personal digital assistant (PDA) with a mobile phone. Later models added the functionality of portable media players, low-end compact digital cameras, pocket video cameras, and GPS navigation units to form one multi-use device. Many modern smartphones also include high-resolution touchscreens and web browsers that display standard web pages as well as mobile-optimized

sites. High-speed data access is provided by Wi-Fi and mobile broadband. In recent years, the rapid developments of mobile app markets and of mobile commerce have been drivers of Smartphone adoption. Smartphones can now operate as small mobile computers by individual users.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. I have received training and experience in the investigation of computer-related crimes. I know all of the below-described information as the result of training and experience in the investigation of computer-related crime and by conferring with other law enforcement personnel who investigate computer-related crime. Much of the information related to computer related crime transfers directly to evidence of crime facilitated by smartphones which are in reality mini-computers.

9. I know that computers, computer technology, and smartphones have revolutionized the way in which child pornography is produced, distributed, and utilized. The advancement in technology of computers, smartphones, and tablets has added to the methods used by child pornography collectors to interact with and sexually exploit children. Each of the above serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. New technology now allows child pornographers to use smaller digital devices, like smartphones and tablets, which have digital cameras and video recording capability built directly into the devices. These devices are equipped with their own processors and memory that allow the devices to actually perform as small mini-computers. With the use of free and publicly available apps, a child pornographer has the ability to produce child pornography, receive and distribute it in a matter of just a few seconds, and

maintain relative anonymity using free open wireless access points.

11. Some device applications operating on the Internet offer their subscribers the ability to communicate publicly or privately with each other in real time in the form of "chat rooms" and/or instant messaging.

12. These communication structures are ideal for individuals who possess, receive, and distribute child pornography. They provide open and anonymous communication, allowing users to locate other persons who share their interest in child pornography, while maintaining their anonymity. Once contact has been established, it is then possible to send text messages, graphic images, and high-resolution video to other individuals interested in child pornography. Moreover, the child pornographer need not use the large service providers. Child pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages are well known and are the foundation of transactions between child pornographers.

13. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution of child pornography. For example, child pornography can be transferred via electronic mail to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services, P2P services, and easy access to the Internet, the computer is a preferred method of receipt

and distribution of child pornographic materials.

14. Based on my knowledge, training and experience, and training and experience of other officers, I know that child pornographers commonly download and save some of their collection of child pornography from their computer to removable media such as smartphones, tablets, iPods or iPads so the images can be maintained in a manner that is both mobile and easily accessible to the collector. Smartphones, iPods or iPads, containing child pornography and printed pictures of child pornography, are not only kept near the computer, but also in hidden areas known to the child pornographer to keep other individuals from discovering the illegal material.

15. Child pornography and evidence of offenses related to child pornography can remain on devices indefinitely unless the user takes active steps to delete or overwrite the child pornography and other evidence of the crimes relating to it.

PROBABLE CAUSE

16. This affidavit is submitted in support of the issuance of a warrant authorizing the search of the property described in Attachment A, including the photographs of the property described in Attachment A, and the digital media, ESI, and data contained within the device. The purpose of the search is the location, seizure, and examination as described in Attachment B.

17. On or about May 5, 2018, an online mobile chat application provider (hereinafter referred to as Application A) notified law enforcement that on May 5, 2018, at 03:39:33 and 03:39:39 UTC, an Application A user with the username "haremking522" accessing the Internet via IP address of 73.120.86.241 distributed two images of child pornography through their servers. Application A provided the two images to law

enforcement. I reviewed the files flagged by Application A and, based on my training and experience, the images depict children, under the age of 18 years old engaged in sex acts and/or lascivious exhibition of their genital areas. The receipt, possession, and distribution of these images violates 18 U.S.C §§ 2252 and 2252A. One of the images is described as follows:

6B32420D344971DAFCA846168760A0F6D9E7FDD4 - This image depicts a young female that appears to be under 12 years of age. The minor female is unclothed and is lying on her back on what appears to be a bed. The minor female is propped up on her right elbow with her legs spread apart. With her left hand, the minor female is holding an erect adult male penis against her vagina.

18. On July 11, 2018, an HSI administrative summons was issued to Comcast for account information relating to IP address 73.120.86.214 on May 5, 2018, at 03:39:33 UTC and 03:39:39 UTC, the IP address, time and date provided by Application A, described above. On or about July 12, 2018, Comcast provided the subscriber as Kristy Holm, 6636 Bay Circle Drive, Knoxville, Tennessee, 37918.

JOSHUA YOUNG'S INTERVIEW AND CONSENT TO SEARCH

19. On August 15, 2018, HSI agents made contact with Joshua Young ("Young"), Kristy Holm's son, at 6636 Bay Circle Drive, Knoxville, Tennessee. Young consented to an interview and to the search of the device. During the interview, Young admitted to having the Application A username "haremking522" and to distributing the two images of child pornography that were flagged by Application A. Young stated a week prior to the interview he had used an online file hosting service (hereinafter the File Hosting Service).¹

¹ Based upon my training and experience, I know that the File Hosting Service referenced by

Young stated he does not have an account with the File Hosting Service, but has links to File Hosting Service accounts that others have shared through Application A chat groups. Young stated on the first page of his phone was a Notes application that contained random links that he goes to. Young stated there are over 10 links for files stored with the File Hosting Service, and the files stored there are a mixture of everything, including child pornography. Young stated his interest in child pornography began in the beginning of May 2017. Young stated he likes both girls and boys age 12 and above and generally likes just poses. Young provided consent for law enforcement to access Young's Application A accounts, but could not remember the passwords. Young provided consent for law enforcement to retrieve his email accounts, but could not remember the passwords. Young consented for HSI agents to maintain possession of his iPhone, further described in Attachment A, for further examination.

20. On August 15, 2018, an HSI Knoxville computer forensics analyst (CFA) further examined the device and observed in the device's web history the key words "PTHC" (preteen hardcore) and "young girl vids," which are known to relate to child pornography. The examination also revealed a list of File Hosting Service links within the Notes application. The Knoxville CFA reviewed one of the File Hosting Service links and found it contained an image with the file name: screenshot_20161011-215934.png, which depicts a female under the age of 18 exposing her genitalia while sitting on a bed.

21. On August 17, 2018, Young contacted HSI agents and withdrew his consent

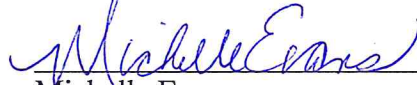
Joshua Young offers cloud storage, file synchronization, and client software. The File Hosting Service allows users to create a special folder on each of their computers, which the File Hosting Service then synchronizes so that it appears to be the same folder (with the same contents) regardless of which device is used to view it. Files placed in this folder also are accessible through a website and mobile phone applications.

to the examination of his iPhone and access to any of his email and social media accounts.

CONCLUSION

22. Based on the aforementioned information, there is probable cause to believe that the device described in Attachment A has been used to violate 18 U.S.C §§ 2252 and 2252A. Further, there is probable cause to believe that evidence, fruits and instrumentalities of those crimes, are presently located on the device described in ATTACHMENT A.

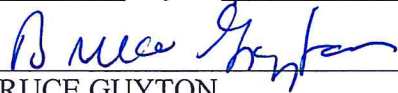
23. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time and to examine, analyze, and test them. Therefore, I respectfully request issuance of the attached search warrant authorizing the search of the device described in ATTACHMENT A and seizure of the items listed in ATTACHMENT B.



Michelle Evans
Special Agent
Homeland Security Investigations

Sworn and subscribed before me

this 1 day of NOVEMBER, 2018



H. BRUCE GUYTON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

Property:

1 white iPhone, Serial Number C8PW4C4PJC6D

Property Location:

The white iPhone is located in the Homeland Security Investigations evidence room located at 324 Prosperity Drive, Knoxville, TN 37923.





ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

All records and information on the devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2252 and 2252A including:

1. Stored image files and video files, including all metadata associated with such files, depicting minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including the lascivious exhibition of the genitalia of minors;
2. Communications, including electronic mail messages, texts messages, social media application messages, and chat room and bulletin board posts, in which child pornography and/or child erotica was discussed or mentioned or by which child pornography was distributed, received, or possessed;
3. Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
4. Records of Internet Protocol Addresses used;
5. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
6. Information identifying persons transmitting, distributing, receiving, or producing any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

